Hindawi
Security and Communication Networks
Volume 2021, Article ID 6966206, 13 pages
https://doi.org/10.1155/2021/6966206

*Research Article*

# Ensuring Improved Security in Medical Data Using ECC and Blockchain Technology with Edge Devices

**Mary Subaja Christo**,[1] **V. Elizabeth Jesi**,[1] **Uma Priyadarsini**,[2] **V. Anbarasu**,[1] **Hridya Venugopal**,[3] **and Marimuthu Karuppiah**[4]

[1]*Department of Networking and Communications (School of Computing), SRM Institute of Science and Technology, Kattankulathur 603203, India*
[2]*Department of Computer Science and Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, India*
[3]*Department of Computer Science and Engineering, Kings Engineering College, Irungattukottai, India*
[4]*Department of Computer Science and Engineering, SRM Institute of Science and Technology, Delhi NCR Campus, Ghaziabad, Uttar Pradesh 201204, India*

Correspondence should be addressed to Mary Subaja Christo; marysubaja@gmail.com

Received 25 July 2021; Revised 28 August 2021; Accepted 4 October 2021; Published 16 October 2021

Academic Editor: Azeem Irshad



Hospital data management is one of the functional parts of operations to store and access healthcare data. Nowadays, protecting these from hacking is one of the most difficult tasks in the healthcare system. As the user's data collected in the field of healthcare is very sensitive, adequate security measures have to be taken in this field to protect the networks. To maintain security, an effective encryption technology must be utilised. This paper focuses on implementing the elliptic curve cryptography (ECC) technique, a lightweight authentication approach to share the data effectively. Many researches are in place to share the data wirelessly, among which this work uses Electronic Medical Card (EMC) to store the healthcare data. The work discusses two important data security issues: data authentication and data confidentiality. To ensure data authentication, the proposed system employs a secure mechanism to encrypt and decrypt the data with a 512-bit key. Data confidentiality is ensured by using the Blockchain ledger technique which allows ethical users to access the data. Finally, the encrypted data is stored on the edge device. The edge computing technology is used to store the medical reports within the edge network to access the data in a very fast manner. An authenticated user can decrypt the data and process the data at optimum speed. After processing, the updated data is stored in the Blockchain and in the cloud server. This proposed method ensures secure maintenance and efficient retrieval of medical data and reports.

## 1. Introduction

In today's world, the healthcare system has an enormous amount of data. These data are very critical and hence their security is a big concern. The critical data related to the patient's health are stored in a file in a conventional method and only a few personal details are stored in the hospital management database. Hence situations that arise when the file is lost are very difficult. To overcome this scenario, a medical health card is used. This card stores all the details of the patient including their medical reports. Hence, the security of this data is very crucial. There are many encryption algorithms to ensure the security of the data and also network security. Choosing the best among them is very important. Hence, a lightweight cryptographic algorithm elliptic curve cryptographic algorithm is used. This algorithm ensures efficient and powerful security of the data with lesser key size compared to other asymmetric cryptographic algorithms. Hence, the memory space is also not wasted. This ensures the confidentiality of the data. Now, these

encrypted data are stored on the Blockchain which is immutable. A Blockchain is as such encrypted by itself. This property provides validation of the data. A block in the Blockchain represents the present data. It has information about past and future data. Every time a block is completed, its transactions are permanent and are stored. The new transactions will be recorded in the current one. Storing of the encrypted data in the Blockchain ensures security and transparency. This enables the feature of authorization to be incorporated to protect the healthcare system. To ensure the fast access of the critical data, these data are stored in the edge server. Hence, this paper focuses on enabling any patient to access their health information from anywhere by card reader, in an efficient manner ensuring confidentiality, integrity, and availability of the critical data.

Now, these encrypted data are stored on the Blockchain which is immutable. Blockchain is a digital ledger that acts as a decentralized database for all transactions. A Blockchain is made up of a series of transactions, each of which is divided into blocks and cryptography keys hold it all together through a hash function. These secret keys are kept in common ledgers and are linked together by a network of nodes. Every node has maintained duplicate data of the entire chain, which is constantly updated and synchronized. A Blockchain is as such encrypted by itself. This property provides validation of the data. A block in the Blockchain represents the present data. It has information about past and future data. Every time a block is completed, its transactions are permanent and stored. The new transactions will be recorded in the current one. Storing of the encrypted data in the Blockchain ensures security and transparency. This enables the feature of authorization to be incorporated in protecting the healthcare system. The following are some of the main concerns with healthcare Blockchain applications:

(1) The member's identities verified and authenticated

(2) Authorization patterns for access to electronic medical records that are consistent

(3) Network infrastructure security at all levels.

Some forms of assaults are possible using Blockchain technology, despite the fact that it has inbuilt protection from others. The code of the Blockchain makes it vulnerable to zero-day attacks and social engineering, as well as defects. As a result, information security must be given special consideration, especially when it is employed in healthcare. All user's information must be kept to the chain. The Blockchain technology has been divided by Public and Private Blockchain. In Public Blockchain, all the data are transparent to all the members, but in Private Blockchain, all the data are transparent to the particular organization. In our research work, we have used Private Blockchain to store the hospital user's data which is transparent to all the members in the hospital and they can view it by Electronic Medical Card.

Our proposed work focuses on the confidentiality of the medical report. To ensure the same, we have kept the encrypted data to the Blockchain which is used for allowing the ethical user to access these data. In edge computing, we can store the medical reports within the edge network; hence, we can access the data in a very fast manner. An authenticated user can decrypt and process the data with optimum speed. After processing, the updated data is stored in the Blockchain and the cloud server. Our proposed method ensures secure maintenance and efficient retrieval of medical data and reports.

The following sections of this paper are prepared as follows. Section 2 describes advance review of EMC and the significance of data security in hospital management systems. The proposed approach to secured medical data using ECC with Blockchain and security measures is explained in Section 3. Security analysis is discussed in Section 4. The performance analysis of the proposed algorithm via simulation algorithm is described in Section 5. Finally, Section 6 describes the conclusion of our proposed work.

## 2. Literature Review

Recent advances in data sharing strategies in the edge computing environment, the importance of Electronic Medical Card in hospital management, the usage of Blockchain technologies in hospital management, and the significance of data security in hospital management systems are briefly covered in this section.

Hema and Kesavan have discussed the importance of e-healthcare in today's world. One of the most difficult challenges in the healthcare system is keeping medical data secure. Elliptical curve cryptography algorithm is used to ensure the main aspects of security, viz, confidentiality and integrity. This also improves the overhead time in various aspects and the insider threat [1]. Tsai et al. have analysed that the ECC requires a lesser key size compared to RSA. This paper discusses ECC-based electronic medical record system that also employs a cloud database. Incorporating an ECC integration unit, a smart card, and a portable device helps to ensure the data transmitted is secure and also the critical data quality is maintained [2]. Vijayakumar et al. have designed IoT-based wearable devices to collect patient medical data and securely pass SMS alerts in medical industry [3, 4].

Poonguzhali et al. have proposed the Blockchain data structure where the data integrity is maintained by making the current data appended to the existing data. These transaction details are maintained by all the nodes that are a part of the network. In this paper, the process consists of two parts: first, the data is kept in the Blockchain and then it is encrypted using the ECC. This enhances the security of the critical data [5]. Jisha and Philip have identified the importance of using elliptical curve cryptography in RFID-based IoT in healthcare systems. The ECC being lightweight and having a lesser key size is much efficient than other asymmetric key algorithms [6]. Bera et al. have developed smart Blockchain Access Control which is used to efficiently detect the hackers in the network communication devices [7]. Karuppiah and Gurunathan have discussed the idea of e-health applications to process the trivial and nontrivial connections among different sensor signals. The data are

stored in the cloud using the "Two Fish Encryption Algorithms" for improved security of the trivial and nontrivial connections among the different sensor signals and big data, the better conception of diseases. Cloud computing provides many benefits, but it also poses significant security risks [8].

Senthilkumar et al. have proposed how data integrity, confidentiality, and authentication is maintained using the Blockchain concept. Here, only authorized users can access the data that is stored in the block. This enables confidentiality and provides security to the critical data [9]. Li et al. proposed Blockchain-based mutual key which provides efficient security communication to vehicles ad-hoc networks [10]. Masood et al. have discussed the security issues of the distributed environment of secured cloud infrastructure [11]. Chaoyang et al. have presented the advantages of elliptical curve cryptography algorithm and also compared this algorithm with nonelliptical curve algorithm. Their work concluded that elliptical cryptography algorithm required small size of bits and provides efficient security to protect any type of data [12].

Shi et al. have presented the review of the edge computing and explained how the processing times are increased with the help of edge devices [13]. Pan and McElhannon have discussed the challenging task of cloud environments. Usually the cloud storage devices required long processing time if the remote database is far and need more computational power. To overcome this challenge, they have suggested the new edge computing system to increase the processing speed of the network and store the computational power of the system [14]. Vijayakumar et al. have proposed secured anonymous and authentication-based intelligent wireless body area networking which provides efficient service to the medical industry [15, 16].

Zhang et al. have integrated the features of edge computing and Blockchain which is used to assure data transfer reliability in the IoT domain and explained how Blockchain and edge computing may be used to create a distributed and trustworthy system with authentication [17]. Hussien et al. have emphasised the incentives for using blockchain machinery in the healthcare systems and addressed the potential challenge of the Blockchain technology [18]. Khatoon et al. have reviewed present Blockchain study in the medical industry and established an Ethereum-based medical management solution and several medical processes are generated for various medical management application domains [19]. Cao et al. have emphasised the need for the edge computing with the developments in the field of IoT. Here, the computations are done at the edge of the network. This increases the processing speed as it is closer to the data and user. The security, protection, and application of the edge networks are discussed [20]. Seo et al. have proposed a certificate less encryption key which is used for sharing the secured information to the cloud. The data holder encrypts the data using the cloud's public key and then the user can upload this secured data to the cloud [21].

Based on the conclusions drawn from the assessment of relevant works, we have proposed secured medical data using ECC and Blockchain technology with edge devices. The ECC algorithm provides excellent performance in all aspects with respect to the time required for file access that includes various steps like key generation, encrypting, and decrypting of the file. To ensure confidentiality and integrity of the critical data, the Blockchain ledger is used to store the encrypted data. To enhance the processing speed of the data, an edge server is added to the cloud-based E-hospital management system.

## 3. Proposed Methodology

In this section, we have enhanced the proposed approach of secured medical data using ECC and Blockchain with edge computing system explained.

*3.1. System Architecture.* As the healthcare system has highly sensitive information that is collected from the patients, it has to be encrypted to preserve security. As the data that are collected are transmitted frequently and is very small, a very lightweight scheme has to be used for encryption. Figure 1 describes the overall architecture of secured hospital management data. The following phases are required to implement our proposed system:

(1) Store user's data in Electronic Medical Card

(2) Encrypt the user's data with elliptic curve cryptographic technique

(3) For encrypted data stored in edge server and Blockchain

  (3.1) edge server allows authenticated management user to process the data

  (3.2) Blockchain technique is used to ensure authentication

(4) Encrypted data is stored in cloud server and authenticated user can view their data from cloud

In the first phase, collect the user's data and store the data on Electronic Medical Card (EMC). The EMC has a microcontroller chip that is used to store user's medical data. Read the data from EMC through the card reader. In the second phase, the elliptic curve cryptography technique has to be used to convert plain text of the medical reports to encrypted text. In the third phase, the encrypted data is stored in edge server and Blockchain which is used to protect our data from hackers or unethical users. The authenticated hospital management users such as doctors, nurses, and admin can decrypt the encrypted data to plain text for further processing with optimum speed. In the fourth phase, authenticated users can retrieve the medical report from the cloud server. Based on these phases, the hospital management can secure the patient's data in smart techniques.

*3.2. Electronic Medical Card.* In hospitals, the patient's health information is stored in their own database and the health records are given back to the patients in a file. In some situation, the manual healthcare reports are not maintained properly and hence the patients may lose the critical data. To avoid these issues, we can use Electronic Medical Card

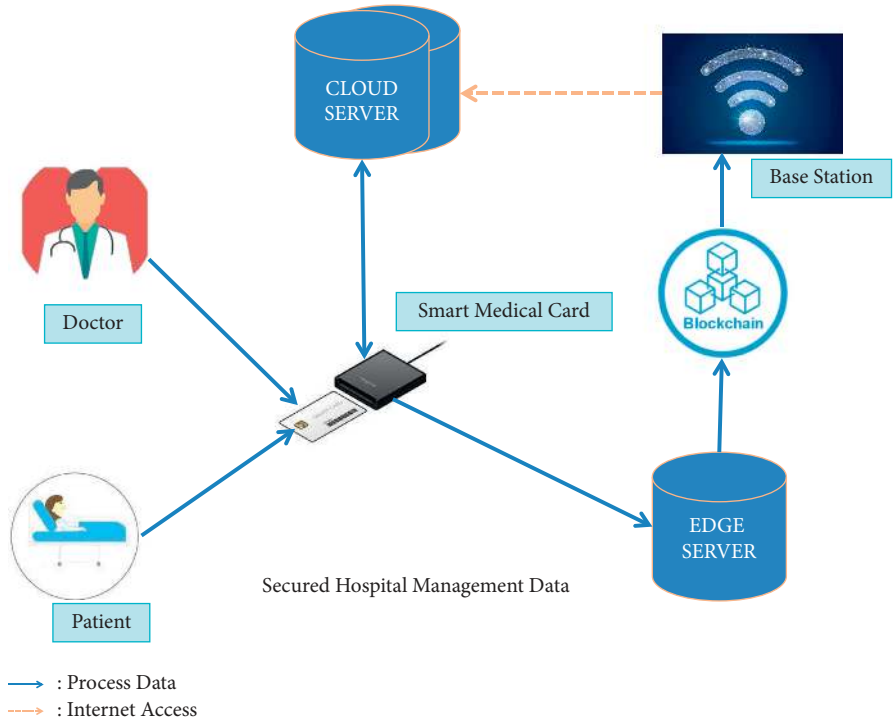


Figure 1: Architecture of secured hospital management.

(EMC), which is used to store medical record in a smart manner. EMC contains an electronic chip which is used to store any kind of medical data to EMC cards. To accomplish this, the patient's registration details are collected from the hospital management system and stored in the electronic chip for smart access. The health-related medical data are retrieved from the IoT sensors like smart watch from the in-patients and out-patients. This information is stored in an EMC card with the help of an electronic chip. This enables the patient medical data to be made available from anywhere at any time.

An EMC is something other than an automated adaptation of a paper outline in a supplier's office. A computerized record can give exhaustive wellbeing data about your patients. EMC frameworks are worked to report data to other medical care suppliers and associations. Figure 2 describes the procedure of the Electronic Medical Card generation. Initially, the hospital management collects basic information from the customer like patients and doctors. The customer basic information and their medical data are stored in EMC. An authenticated user can access their card. So initially, the EMC card can be activated by the user's DOB or their PAN card number. After login, they can reset their password credentials for further processing. EMC is also connected to the hospital local base station. So it helps the patient to check their medical status themselves. The medical data is updated to EMC by the healthcare sensor which is embedded in the patient's body.

*3.3. Encrypt the Medical Data with Elliptic Curve Cryptography Algorithm.* Hospital management should secure their user-related data such as patient's basic information, medical data, and medicine description. Today, securing the user data is the utmost challenge that hospital management faces. In this paper, we have proposed elliptical curve cryptography (ECC) algorithm for the encryption and decryption process. ECC is an asymmetric algorithm that uses two keys, that is, the private key and public key, for encryption and decryption. The difference between the ECC algorithm and non-ECC algorithm is that ECC provides equal security with smaller key size as compared to non-ECC algorithms such as RSA and DSA. As the name suggests, the ECC algorithm uses elliptic curves. Elliptic curves are defined by some mathematical functions which are cubic functions which is the equation of degree 3. The equation of the elliptic curve is $Y^2 = X^3 + (A * X) + B$, where the coordinates of the elliptic curve equation is $((X_1, Y_1), (X_2, Y_2)$----) [8].

*3.3.1. ECC Algorithm.* ECC the algorithm is used to encrypt the plain text to cypher text. To implement ECC key exchange, we need global public elements which have 2 parameters. The first element is $Eq$ $(c, d)$ where $E$ is an elliptic curve, $E$ $(c, d)$ is an elliptic curve with constants $c$ and $d$, and $q$ is the prime number or an integer of the form 2M [8]. The second element is $G$ which is a point on the elliptic curve. In this key exchange algorithm, we have considered two users: user $A_1$ and user $B_1$. Next, we generate private key and public key for User $A_1$ and User $B_1$ after generating the private and public keys. We generate the secret key which is shared by both user $A_1$ and user $B_1$. Figure 3 describes the flowchart to generate the EMC card for smart hospital management.

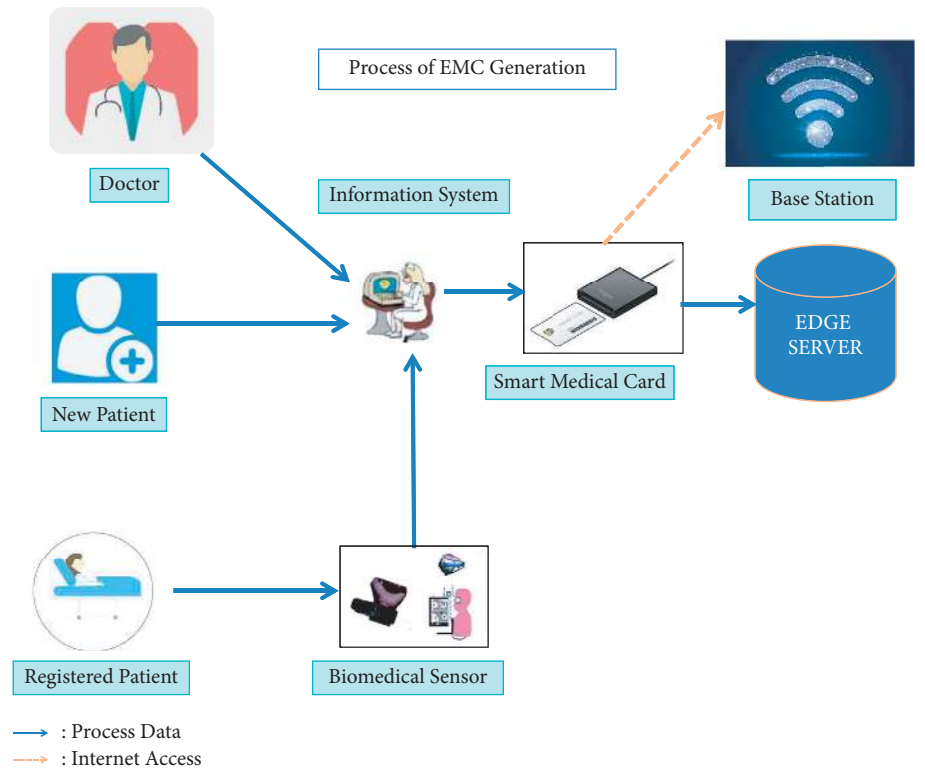


Figure 2: EMC generation.

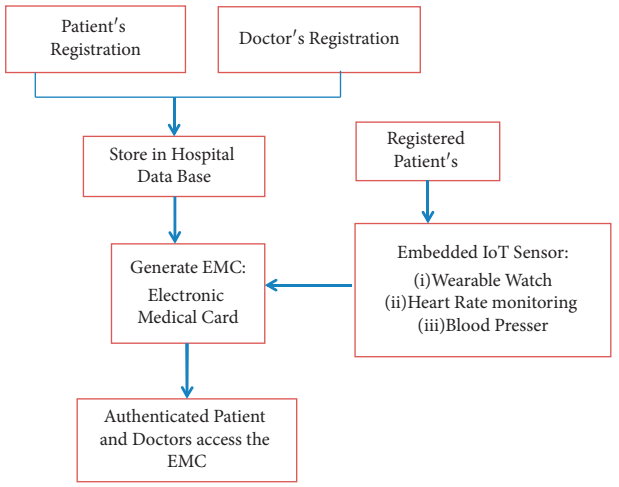


Figure 3: Flowchart to generate the EMC of hospital users.

The following phases are used to implement this algorithm:

(1) ECC key exchange

(2) Key generation at user $A_1$ and user $B_1$

(3) Secret key generation at user $A_1$ and user $B_1$

(4) ECC encryption

(5) ECC decryption

Table 1 describes the comparison of the ECC algorithm and non-ECC algorithm like RSA and DSA. ECC algorithm provides equal security as RSA and DSA with smaller key sizes. So this algorithm requires a minimum amount of memory and computational power than non-ECC algorithms [22].

Table 1: Comparison of ECC and non-ECC algorithm.

| Minimum size (bits) of public key | | |
|---|---|---|
| DSA | RSA | ECC |
| 1024 | 1024 | 160 |
| 2048 | 2048 | 224 |
| 3072 | 3072 | 256 |
| 7680 | 7680 | 384 |
| 15360 | 15360 | 512 |

*3.3.2. ECC Algorithm-Based Encrypted and Decrypted Hospital User's Data.* The following parameters are used to encrypt and decrypt hospital user's data:

*E- > Eq* $(x, y)$ *Let E, n,* and $q$ be elliptic curve, curve value limit, and random number, respectively.

*Let* $x$ and $y$ be constant parameters.

*Let G* and *K* be elliptic curve point and random positive number, respectively.

*Let HA* and *HU* be hospital admin and hospital user, respectively.

*Let* $n_{HA}$, $p_{HA}$, and $k_{HA}$ be the private, public, and secret key of hospital admin.

*Let* $n_{HU}$, $p_{HU}$, and $k_{HU}$ be the private key, public key, and secret key of hospital user.

*Let PT, p, d,* and *CP* be the plain text, patients' data, doctors' data, elliptic curve point, and cipher point.

*Let* $EP_{PT}$ be encoding plain text to elliptic curve point.

*Compute Z < - MUL* (*X*) coordinate with *HU* private key.

*3.4. Blockchain Ledger with ECC Encrypted Data.* A Blockchain is as such encrypted by itself. This property provides validation of the data. A block in the Blockchain represents the present data. It has information about past and future data. Every time a block is completed, its transactions are permanent and stored. The new transactions will be recorded in the current one. Storing of the encrypted data in the Blockchain ensures security and transparency. This enables the feature of authorization to be incorporated in protecting the healthcare system. Distributed Ledger Technology is a decentralized database that is administered by various people (DLT). This means that if a single block in a chain is modified, it will be immediately clear that the chain has been tampered with. Hackers would have to change every Block in the chain, across all distributed versions of the chain, if they intended to destroy a Blockchain system.

The Blockchain is one of the stored devices in which a new record is added to the previously stored record and is transparent to all the members in the network. The healthcare industry is currently concentrating on the efficient Blockchain design to keep the hospital user's data more safe, confident, reliable, and distributed, as they are in the existing file system incapable to maintain the confidentiality and reliability of the information. The goal of the proposed effort is to use Blockchain to store the encrypted hospital user data which is read from the EMC. Our proposed framework helps to increase the confidentiality of all the hospital users like patients, doctors, etc. The following are the major aspects of Blockchain technology:

(1) Immutable: once updated, we cannot alter the records

(2) Distributed: duplicate data are kept in all the devices in the same network so any member can view their data

(3) Consensus: every block is validated by a member of the network's miner

(4) Transparent: all network members have access to the data and may observe the data

*3.4.1. Blockchain Ledger.* Each node in the Blockchain system is going to uphold a record for all the communications and these transactions are going to maintain the state of the data that is being stored on the Blockchain network and the ledger often consists of two types of data structures. The first data structure is Blockchain itself so this is an append-only log of all transactions that have happened; it is similar to a linked list of blocks and a block is a group of transactions that have been put together. As we know, the linked lists are blocked and they are linked with each other with a hash value that is computed on each block. A part of the next block is known as a hash chain. So in every block of transactions, there is a cache of it that is computed and that hash is added on to the next block that is about the hash chain. This Blockchain gives some certain properties of immutability. If you modified or tampered with a previous block, then the hash on the next block will not match. So it will be very hard for someone to tamper with the previous block and also these blocks are maintained in a decentralized fashion, which means that we will take down or manipulate a large net number of nodes in the network, and a large fraction of nodes in the network will be possible to tamper with, so it gives a lot of immutability properties. This is known as the Blockchain aspect of the ledger. So this is the sequence of transactions that each node in the system is going to uphold the data. It stores the most recent state of smart contracts that are the outputs of each transaction and the data elements can be added, modified, deleted, and all recorded as transactions on Blockchain. In our proposed work, we have used the first type of ledger that is the Blockchain ledger data structure.

The proposed Blockchain architecture with EMC data processing of the system is described in Figure 4. The design covers how to initiate a connection and how to add or create a new block to the existing block. To begin the connection, the member, who could be any of the EMC system's stakeholders, sends a new message stating that a block or record has been formed. This recently produced block or record may comprise a doctor's investigation, a lab technician's test report, a nurse's pressure reading, a pharmacist's medication, and so on, which is distributed to all devices connected in the network via the Blockchain. The transaction is kept within the block and published to all network nodes.

After the Blockchain is complete, all nodes in the network have a similar copy of data, allowing members to collaborate during the verification process. They authenticate that the block containing the transactions is unchanged as soon as it is broadcast to all members of the network. Once the verification process is completed, the new node is appended to the previous block. Each block on the Blockchain is made up of three components: data, the current block's hash value, and the previous block's hash value. The information regarding the patient's health is stored in the suggested system's data. Our proposed Blockchain ledger with ECC algorithm is used to ensure the confidentiality of the hospital user data.

*3.5. Processing of Data Storage in Edge Device.* In edge computing, we can store the medical reports within the edge network; hence, we can access the data in a very fast manner. An authenticated user can decrypt and process the data with optimum speed; after processing, the updated data has been stored to the Blockchain and the cloud server. Figure 5 shows the encrypted data are kept in the Blockchain ledger to improve confidentiality. Next, these encrypted data are stored in the edge server to continue further data processing. If the doctor wants to check his patient's data, he should log

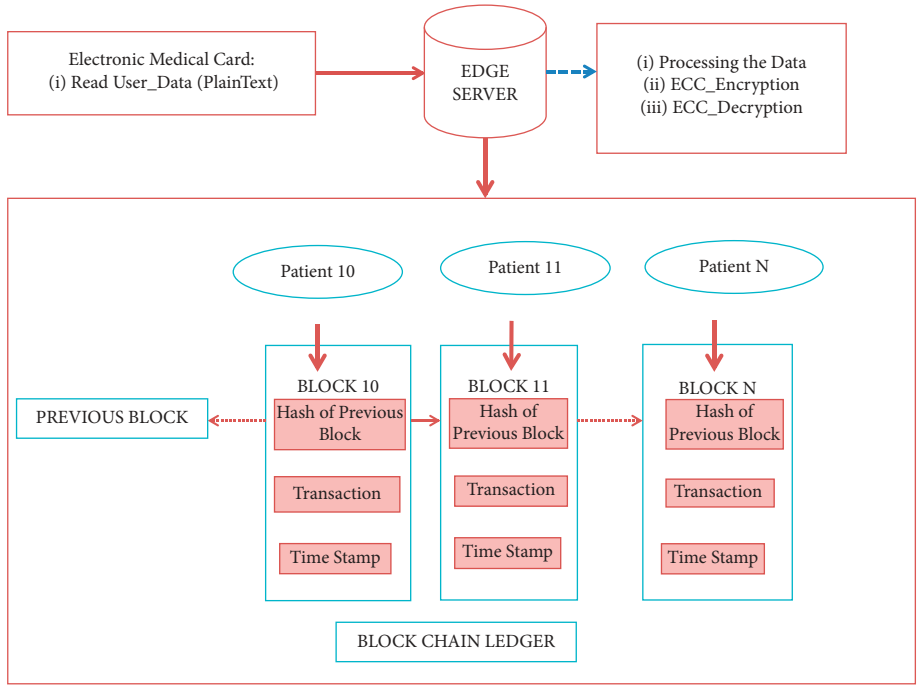


Figure 4: EMC data processing in Blockchain.

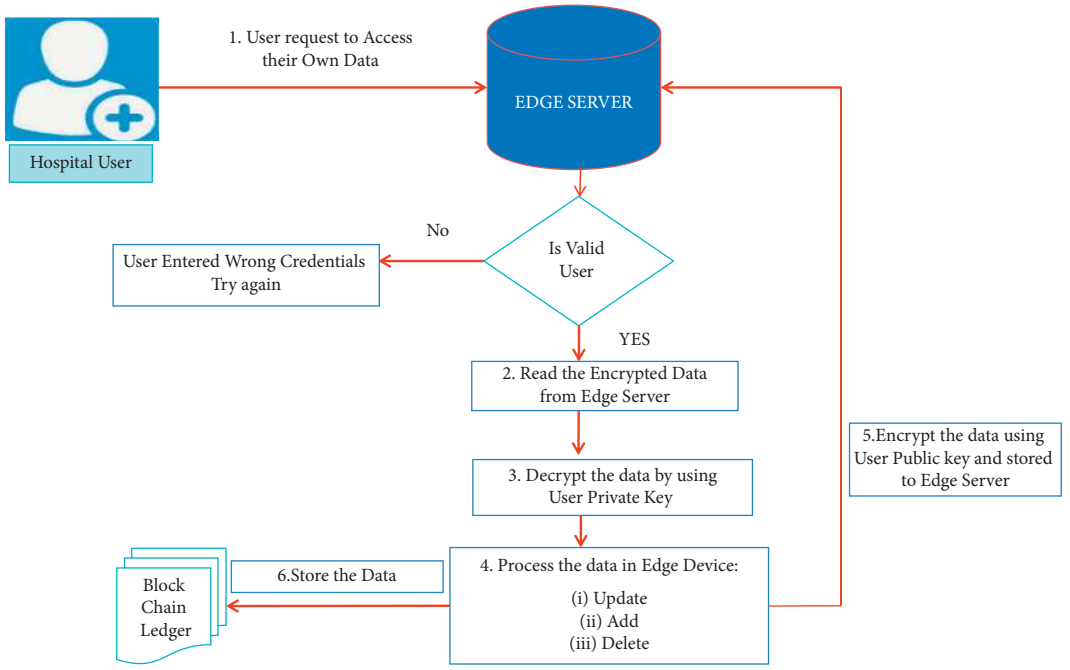


Figure 5: Optimum data processing in edge server.

in with an Electronic Medical Card with his credentials after validating his request, and he can decrypt the patient data with his private key which is described in the ECC algorithm module. Once processing has completed, the doctor again keeps the data to the Blockchain in a separate block with the previous hash value of the patient.

Edge computing was established to allow cloud resources and services to be deployed at the network's edge. However, it presently faces issues in terms of management and security due to its decentralized nature. Edge computing offers the ability to address issues such as reaction speed, battery life, and bandwidth cost savings, as well as data security and privacy. In the last several years, the volume of data generated by sensors, actuators, and other devices on the Internet of Things (IoT) has skyrocketed. Data from IoT devices are currently handled via the cloud, primarily using computing resources in remote data centres. Figure 5 shows the optimum speed of data processing of hospital user data.

As we know, edge computing is used to store the data in edge devices so we can process our data at high speed, low bandwidth, and quick response.

To optimise computation and storage resources, edge computing nodes are used. In the hospital, if the doctor wants any emergency data of the patient, he can access the data within a fraction of a second. After processing in edge devices, the data are stored into the cloud server. Now all the required hospital data are stored in the cloud and at any time the user can access their data by himself and the doctors can efficiently track the patient's details. Hence our proposed work helps to protect hospital data, provides the optimum speed of processing the data, provides the users with the ability to check their data by themselves, and increases the computational power and storage capacity.

*3.6. The Proposed Algorithm: Edge Server and Blockchain-Based Secured Hospital User Data with ECC Algorithm.*

(1) START

(2) **For** each user get User name and Password

(2.1) **IF** User is authenticated

(2.1.1) **Do** Access to Use EMC card
(2.1.2) **Go** to the Step3

(2.2) **Else** Invalid User

(2.2.1) **Invalid** User
(2.2.2) **Exit**

(3) **Store** Data to EMC card

(4) **Read** Plain text (Data)

(5) **Start** ECC Encryption Process in Edge Server

(5.1) **Generate** the Public Key and Private Key by Algorithm 1
(5.2) **Do Encryption** Process by Algorithm 2

(6) Request for Decryption Process in Edge Server

(6.1) **If** Authenticated User
(6.2) **Do Decryption** Process by Algorithm 3

(7) Data Stored in Blockchain and Cloud Server

(8) Every Authenticated User View their Own Data

(9) **STOP**

The proposed algorithm is used to secure the EMC by securing the data using the lightweight ECC technique in edge server database and the block chain concept ensures the data is more secured.

## 4. Security Analysis

Every user's *HA* and *HU* are authenticated by 2-layer protection. To change the password initially, the user is asked to enter the PAN card number to validate the user along with the user name. Once the user is validated, an autogenerated message is sent to the user's registered phone number. Clicking on the message which consists of hyperlink validates the user. Hence the user is double authenticated to change the password. The security features provided in the proposed system are essentially sustained by cryptography algorithms and hash functions. The following subsection discusses threats, security issues, challenges, and solutions for different kinds of attacks in the proposed system.

*4.1. Password Guessing Attack.* Password guessing attack is also known as brute force attack. An attacker can easily guess the password with certain combinations of user credentials. Therefore, passwords should be set strongly to avoid this attack. Every registered *HA* and *HU* should create their password by adhering to the following rules: password should contain a minimum of 10 characters to strengthen the security. Password should contain at least two uppercase alphabets, 2 numbers, and 2 special characters. This constraint is validated against the password while setting the password.

*4.2. Man-in-the-Middle Attack.* In this approach, the hacker may be able to deceive both shared entities while retaining none of their sensitive information. The proposed system uses an ECC algorithm that encrypts the *HU* and *HA* user's data. *PT* is encrypted as $CPPT = \{K*G, EPPT + K*pHU\}$. The encrypted data is stored in Blockchain with the hash key values. The user is encrypted twice using the encryption key and hash key. Therefore, the proposed algorithm achieves dual encryption. If any attacker who is in between the hospital and user attempts to alter a hospital user's message, the key does not match with the decrypted message which is given as $HU <\text{-}\ EPPT + K*\ pHU\ \text{-}\ K\ *\ pHU$.

*4.3. Message Modification Attack.* The integrity of the suggested approach is protected from harmful usage. To maintain integrity, Blockchain maintains a chain connection by linking the previous block value with the current block value. If an attacker attempts to change a block value, the same will be cross verified with the entire block. Therefore, the distributed Blockchain data identifies the attacker and alerts the HA and HU. Hence our proposed Blockchain-based method does not allow message modification attacks.

*4.4. Reply Attack.* In this proposed approach, the attacker can delay the message sent between the *HA* and the *HU*. However, if the communication is overdue, the attached timestamp will be unacceptable. Then the communication will be unauthenticated. If the timestamp is not correct, the hospital administrator just discards the notification without taking any further action. A legitimate session key can be disrupted by an opponent $(K = HU, T1, F(HU, T1))$ and again sent to the user. The hospital admin checks the timestamp value and if the timestamp value is not equal to T1, the message is rejected by the hospital admin. Even if the attacker generates a fresh timestamp, the hash value cannot be manipulated by the attacker. Finally, the message will be rejected by the hospital user. Hence, the replay attack is invalid in our proposed system.

**Input:** Hospital User (*HU*) data; Key size: 516 bits
**Output:** public, private and secret key of *HU* & *HA*
(1) **create** $E$
(2) **generate G**
(3) **for-each** Hospital User (*HU*) do;
(4) **create** private key and public key of *HA*
(4.1) **create** private key ($n_{HA}$) of *HA*; where $n_{HA} < n$
(4.2) **compute** public key ($p_{HA}$) of *HA*; where $p_{HA} = n_{HA}(G)$
(5) **create** private key and Public key of *HU*
(5.1) **create** private key ($n_{HU}$) of *HU*; where $n_{HU} < n$
(5.2) **compute** public key ($p_{HU}$) of *HU*; where $p_{HU} = n_{HU} * G$
(6) **create** secret key of *HA*; $k_{HA} = n_{HA} * p_{HU}$
(7) **create** secret key of *HU*; $k_{HU} = n_{HU} * p_{HA}$
(8) **end** for-each;

Algorithm 1: Key generation: *HU* & *HA*.

**Input:** plain text (*PT*)
**Output:** cipher text ($CP_{PT}$)
(1) **read** *PT*
(2) **encode** $PT -> EP => EP_{PT}$
(3) **compute** *CP*
(3.1) **compute** $CP_{PT}$; $CP_{PT} = \{K*G, EP_{PT} + K*p_{HU}\}$
(3.2) **compute** X-coordinate = $K*G$; Y-coordinate = $EP_{PT} + K*p_{HU}$

Algorithm 2: *HA* - ECC encryption process.

**Input:** Cypher text
**Output:** Plain text
(1) **get** cipher point ($CP_{PT}$) at receiver end
(2) **compute** $Z = KG * n_{HU}$
(3) **subtract** $Z$ from $Y$ coordinates and **compute** the following:
(3.1) $HU <- EP_{PT} + K*p_{HU} - (Z)$
(3.2) $HU <- EP_{PT} + K*p_{HU} - (KG * n_{HU})$
(3.3) $HU <- EP_{PT} + K* p_{HU} - K * p_{HU}$ *where* $p_{HU} = n_{HU} * G$
(3.4) $HU <- EP_{PT}$

Algorithm 3: *HU* - ECC decryption process.

## 5. Performance Evaluation

*5.1. Setup for Experiments.* In this paper, we have proposed to improve the security level of the hospital user's data. Our proposed system has four major entities, as explained in the system model that stores the user's data to EMC: use ECC encryption algorithm to secure the data, use Blockchain to store the encrypted data to ensure the confidentiality and integrity of the data, and use the edge server to process the secured data which is used to increase the transmission rate, reduce the computational power, increase the computational memory, etc. Finally the encrypted data are stored in the cloud. We have done our experiments in MAT LABR 2008a on Intel(R) Core(TM) i5-1035G1 CPU @ 1.00 GHz 1.19 GHz with 8.00 GB (7.79 GB usable) under Ms-Windows platform. The following characteristics are used to assess the system's performance: time for key generation, time for data encryption, time for data decryption, time for data upload, time for data download, file processing speed, and cost of security.

*5.2. Results of Experiments*

*5.2.1. Time Required for Key Generation.* Key generation time is the amount of time it takes to generate keys in cryptography. The created key is used for the encryption process and decryption process. In this system, the key generation time is estimated for a set of hospital users ranging from 10 to 100 users at a time interval of 10 units. Figure 6 shows how much amount of time is required for key generation based on ECC and non ECC algorithms. As

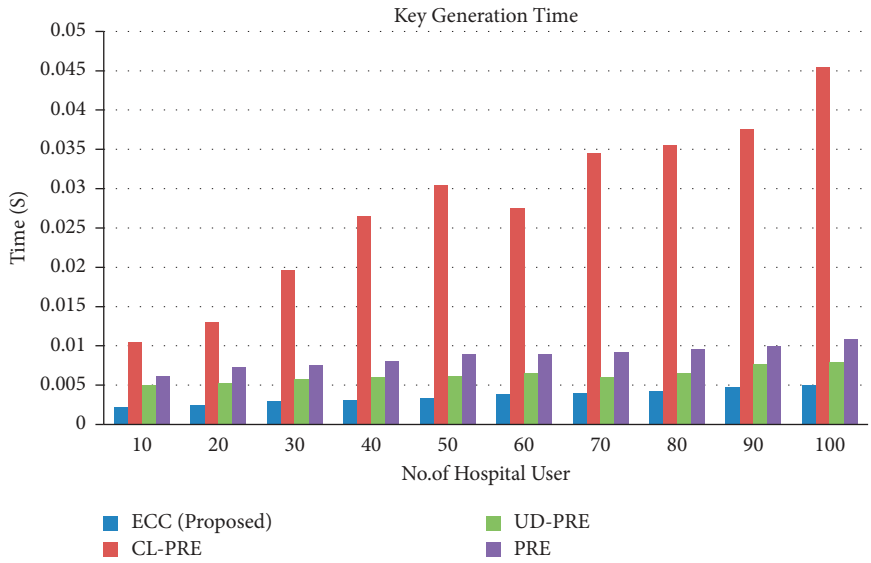


Figure 6: Comparison of key generation ECC with non-ECC algorithms.

expected, the key generation time increases as the number of hospital users increases. The time spent on key creation is not proportionate to the growth of hospital users, according to the data. The time usage for key generation barely differs by 0.005 seconds as the number of hospital users increases from 10 to 100. The amount of time it takes to generate a key varies only by 0.005 seconds.

Table 2 shows a detailed comparison of key generating methods with ECC and non-ECC an algorithm like a Certificate Less Proxy Reencryption (CL-PRE) scheme [23], Unidirectional Proxy Reencryption (UD-PRE) schemes [24], and Proxy Reencryption (PRE) [25]. The ECC is more substantial than other non-ECC compare methods, according to this observation.

*5.2.2. Processing Time of ECC with Blockchain.* The file encryption time is defined as the time it takes the hospital administrator to encrypt a file. To calculate the computational cost of processing a file, how much time is required to convert plain text to cypher text which means file encryption time and how much time is required for convert cypher text to plain text which means file decryption time and secret key generation time are taken into account. The time it takes to encrypt files of various algorithms like ECC and non-ECC is depicted in Figure 7.

The statistic for encryption time demonstrates when computation time of ECC algorithm is compared with non-ECC algorithms. ECC required minimum amount of time to encrypt and decrypt the file as key size is 516 bits.

The decryption result has a similar tendency to that of encryption. It also demonstrates that key computation time has no effect on file size, which remains constant even with minor alterations.

In ECC, the entire time spent computing encryption key varies between 0.020 and 0.0195 seconds. Table 3 shows detailed computation time values of encryption time, encryption key generation time, decryption time, and decryption key generation time with various cryptographic algorithms. The file decryption time in this ECC with a Blockchain-based system is defined as the time it takes the hospital user to decrypt a file based on his request from the Electronic Medical Card.

*5.3. Processing the Data in Edge Server.* In edge computing, we can store the medical reports within the edge network; hence, we can access the data in a very fast manner. An authenticated user can decrypt the data and process the data with optimum speed. After processing, the updated data has been stored to the Blockchain and the cloud server.

The entire time it takes to upload a file to edge server as well as download a file from the edge, the server is also used to evaluate the suggested methodology's performance. The following components make up the total time: (i) secret key generation time, (ii) time taken converting plain text to cypher text or decryption, (iii) time taken to upload the file to edge server or download a file from edge server, and (iv) total time required for all communications like get request time from hospital user through Electronic Medical Card and response time for uploading or downloading the file. Figure 8 shows the file upload time process performance as a function of file size.

As the size of a file grows larger, the time it takes to upload it to the health edge server and cloud grows longer. The file downloading procedure is the inverse of the uploading process, in which the hospital administrator obtains the original data file. The download time varies depending on the input size and bandwidth of the network. The download time increases gradually as the input size of the file increases from 10 to 250 MB.

Table 4 shows how much amount of time is required to upload file to edge server and cloud server and how much amount of time is required to download the file from edge

Table 2: Key generation value of ECC and non-ECC algorithms.

| | Key generation time (S) | | | |
|---|---|---|---|---|
| No of users | ECC (proposed) | CL-PRE | UD-PRE | PRE |
| 10 | 0.00222 | 0.0105 | 0.005 | 0.00621 |
| 20 | 0.00245 | 0.013 | 0.00525 | 0.00735 |
| 30 | 0.00296 | 0.0196 | 0.00576 | 0.007592 |
| 40 | 0.00306 | 0.0265 | 0.006 | 0.00802 |
| 50 | 0.00338 | 0.0305 | 0.00612 | 0.008935 |
| 60 | 0.00389 | 0.0275 | 0.0065 | 0.00892 |
| 70 | 0.00402 | 0.0345 | 0.0061 | 0.00927 |
| 80 | 0.00429 | 0.0355 | 0.00652 | 0.00963 |
| 90 | 0.00473 | 0.03758 | 0.00764 | 0.00999 |
| 100 | 0.00498 | 0.0455 | 0.0079 | 0.010810 |

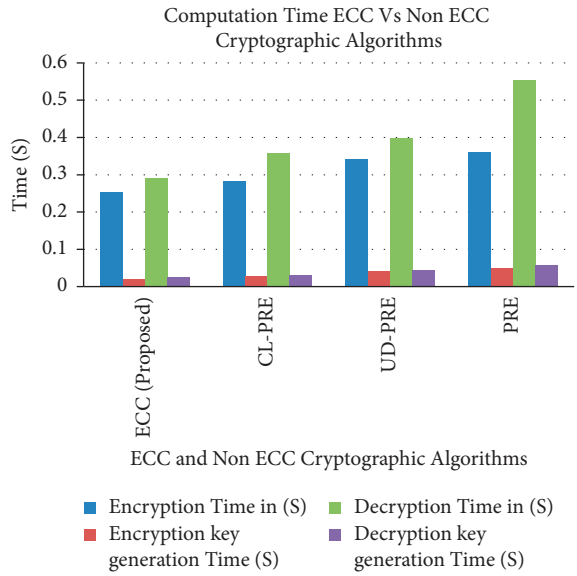


Figure 7: Time consumption with various input file size.

Table 3: Encryption and decryption time with various algorithms.

| Cryptography algorithms | Encryption time in (S) | Encryption key generation time (S) | Decryption time in (S) | Decryption key generation time (S) |
|---|---|---|---|---|
| ECC (proposed) | 0.2533 | 0.021 | 0.2900 | 0.0256 |
| CL-PRE | 0.2833 | 0.029 | 0.3566 | 0.0314 |
| UD-PRE | 0.3422 | 0.043 | 0.3995 | 0.0455 |
| PRE | 0.3599 | 0.050 | 0.5533 | 0.0589 |

server and cloud. The result also shows that the upload and download speed are nearly consistent, with only 1 Mbps difference over the calculated range of 10 to 250 MB.

*5.4. Security Level of the System.* Based on our analysis, the proposed system provides more security to hospital user's data. There may be a delay in the system if the hospital management uses only the cloud to upload and download the file. We have proposed edge-based system to upload and download the file so the hospital users can process the data at an optimum speed based on the size of the input files, which provides a high-security level to our system as we used ECC-based encryption algorithm and the encrypted user's data are stored in the Blockchain to increase the confidentiality and integrity of the system.

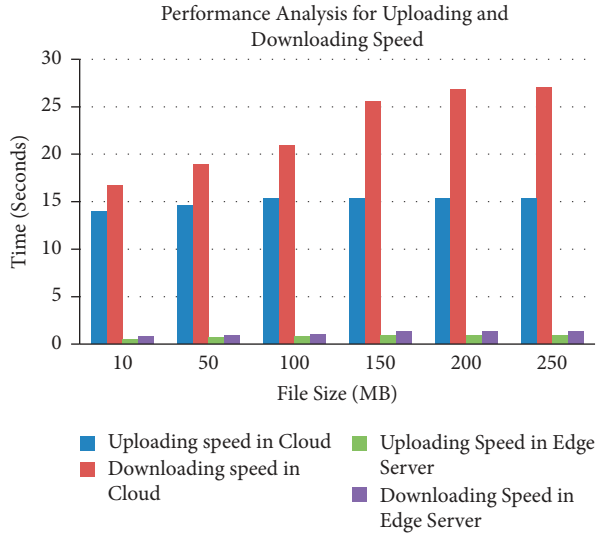


Figure 8: Downloading speed with respective edge server and cloud server.

Table 4: Downloading speed with edger server vs cloud server.

| File size | Uploading speed in cloud | Downloading speed in cloud | Uploading speed in edge server | Downloading speed in edge server |
|---|---|---|---|---|
| 10 | 13.93 | 16.68 | 0.513 | 0.759 |
| 50 | 14.567 | 18.956 | 0.6567 | 0.867 |
| 100 | 15.345 | 20.893 | 0.757 | 0.958 |
| 150 | 15.345 | 25.567 | 0.857 | 1.343 |
| 200 | 15.345 | 26.789 | 0.857 | 1.343 |
| 250 | 15.345 | 26.999 | 0.857 | 1.343 |

## 6. Conclusion

Maintaining, securing, and sharing medical data of patients in hospitals are a considerable challenging situation for hospital management. Invasion of patient privacy data should be strictly limited to authorized users. There are various privacy concerns that may hinder the data in which patient privacy could be abused. To handle these privacy concerns, the proposed framework uses an enhanced security methodology for sharing patient's and doctor's medical information with health management in a secured way. The proposed methodology uses a framework that stores the data in EMC. This card stores information like patient personal information, medical record, and consultation details. The information stored in the card is secured using the ECC algorithm. The algorithm uses the key to encrypt and decrypt the data. The data of the end-users are stored efficiently in cloud infrastructure. This mechanism provides more flexibility in viewing the medical data at any period of time. The experimental results reveal that the time taken to generate the key, encryption, and decryption is improved compared to other existing algorithms. The proposed framework also offers edge servers at the ground to process the data effectively and store the data in cloud servers. This research ensures not only data security but also data confidentiality and authenticity by processing and storing the data in the Blockchain ledger.

## Data Availability

Basic information of patients and doctor and medical data of patients are used in the study.

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## References

[1] V. S. V. Hema and R. Kesavan, "ECC based secure sharing of healthcare data in the health cloud environment," *Wireless Personal Communications*, vol. 108, 2019.

[2] K. L. Tsai, F.-Y. Leu, T.-H. Wu, S.-s. Chiou, Y.-W. Liu, and H.-Y. Liu, "A secure ECC-based electronic medical record system." *Journal of Internet Services and Information Security*, vol. 4, no. 1, pp. 47–57, 2014.

[3] P. Vijayakumar, P. Pandiaraja, M. Karuppiah, and L. Jegatha Deborah, "An efficient secure communication for healthcare system using wearable devices," *Computers & Electrical Engineering*, vol. 63, pp. 232–245, 2017.

[4] P. Vijayakumar, S. M. Ganesh, L. J. Deborah, and B. S. Rawal, "A new SmartSMS protocol for secure SMS communication in m-health environment," *Computers & Electrical Engineering*, vol. 65, pp. 265–281, 2018 Jan 1.

[5] N. Poonguzhali, S. Gayathri, A. Deebika, and R. Suriapriya, "A framework for electronic health record using blockchain technology," in *Proceedings of the 2020 International*

*Conference on System, Computation, Automation and Networking (ICSCAN)*, 3 July 2020.

[6] S. Jisha and M. Philip, "Rfid based security platform for internet of things in health care environment," in *Proceedings of the 2016 Online International Conference on Green Engineering and Technologies (IC-GET)*, IEEE, Coimbatore, India, 19 Nov. 2016.

[7] B. Bera, A. K. Das, M. Obaidat, P. Vijayakumar, K. F. Hsiao, and Y. Park, "AI-enabled blockchain-based access Control for malicious attacks detection and mitigation in IoE," *IEEE Consumer Electronics Magazine*, vol. 10, 2020.

[8] S. V. Karuppiah and G. Gurunathan, "Secured storage and disease prediction of E-health data in cloud," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, 2020.

[9] D. Senthilkumar, "Data confidentiality, integrity, and authentication." in *Research Anthology on Blockchain Technology in Business, Healthcare, Education, and Government*, pp. 459–487, IGI Global, Hershey, PA, USA, 2021.

[10] X. Li, Y. Wang, P. Vijayakumar, D. He, N. Kumar, and J. Ma, "Blockchain-based mutual-healing group key distribution scheme in unmanned aerial vehicles ad-hoc network," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11309–11322, 2019.

[11] I. Masood, Y. Wang, A. Daud, N. R. Aljohani, and H. Dawood, "Towards smart healthcare: patient data privacy and security in sensor-cloud infrastructure," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[12] Z. Chaoyang, "Elliptic Curve Arithmetic in onion routing anonymity networks,"vol. 6, pp. 130–134, in *Proceedings of the In2010 3rd International Conference on Computer Science and Information Technology*, vol. 6, , IEEE, Chengdu, China, 2010 Jul 9.

[13] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: vision and challenges," *IEEE internet of things journal*, vol. 3, no. 5, pp. 637–646, 2016.

[14] J. Pan and J. McElhannon, "Future edge cloud and edge computing for internet of things applications," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 439–449, 2017.

[15] P. Vijayakumar, M. S. Obaidat, M. Azees, S. H. Islam, and N. Kumar, "Efficient and secure anonymous authentication with location privacy for IoT-based WBANs," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, pp. 2603–2611, 2019.

[16] F. Wei, P. Vijayakumar, J. Shen, R. Zhang, and L. Li, "A provably secure password-based anonymous authentication scheme for wireless body area networks," *Computers & Electrical Engineering*, vol. 65, pp. 322–331, 2018.

[17] P. Zhang, X. Pang, N. Kumar, G. Singh Aujla, and H. Cao, "A reliable data-transmission mechanism using blockchain in edge computing scenarios," *IEEE Internet of Things Journal*, 2020.

[18] H. M. Hussien, S. Md Yasin, N. I. Udzir, M. I. Hafez Ninggal, and S. Salman, "Blockchain technology in the healthcare industry: trends and opportunities," *Journal of Industrial Information Integration*, vol. 22, Article ID 100217, 2021.

[19] A. Khatoon, "A blockchain-based smart contract system for healthcare management," *Electronics*, vol. 9, no. 1, p. 94, 2020.

[20] K. Cao, Y. Liu, G. Meng, and Q. Sun, "An overview on edge computing research," *IEEE access*, vol. 8, pp. 85714–85728, 2020.

[21] S.-H. Seo, M. Nabeel, X. Ding, and E. Bertino, "An efficient certificateless encryption for secure data sharing in public clouds," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 9, pp. 2107–2119, 2014.

[22] E. Vidhya, S. Sivabalan, and R. Rathipriya, "Hybrid key generation for RSA and ECC," in *Proceedings of the 2019 International Conference on Communication and Electronics Systems (ICCES)*, pp. 35–40, IEEE, Coimbatore, India, 2019 Jul 17.

[23] L. Xu, X. Wu, and X. Zhang, "CL-PRE: a certificates proxy re-encryption scheme for secure data sharing with public cloud," in *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, pp. 87-88, Seoul, South Korea, 2012.

[24] Y. R. Chen, J. D. Tygar, and W. G. Tzeng, "Secure group key management using uni-directional proxy re-encryption schemes," in *Proceedings of the IEEE INFOCOM*, pp. 1952–1960, IEEE, Shanghai, China, 2011 Apr 10.

[25] A. N. Khan, M. L. M. Kiah, S. A. Madani, M. Ali, A. u. R. Khan, and S. Shamshirband, "Incremental proxy re-encryption scheme for mobile cloud computing environment," *The Journal of Supercomputing*, vol. 68, no. 2, pp. 624–651, 2014.